Informatique Quantique
&
Blockchain

Le futur ?

L’informatique quantique

L’informatique quantique

Qu’est ce que le quantique ?

Branche de la physique qui traite des propriétés des quantons (bosons & fermions)

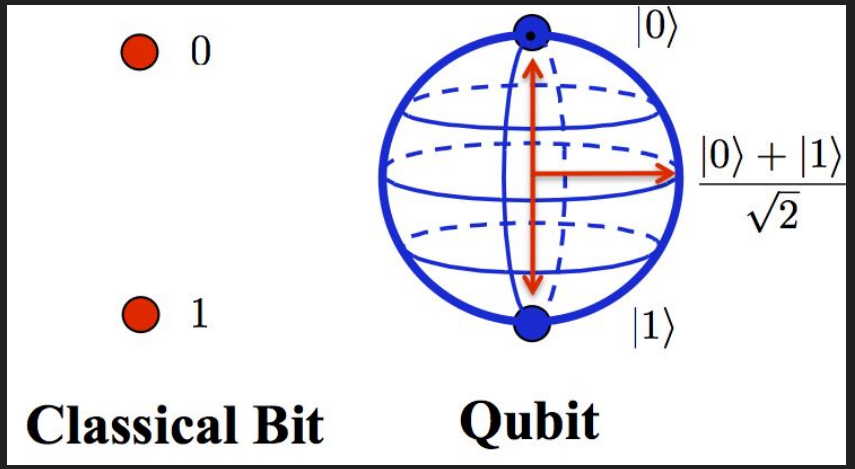
Quanton(1967) : “Objet physique que l’on peut dénombrer mais pas spatialiser précisément”

Bits et Qubits

Qubits : Quantum Bits

Un quantum bit ou qubit va pouvoir prendre via le principe de superposition :

une combinaison linéaire $a|0\rangle + b|1\rangle$ $(a,b) \in \mathbb{C}^2$



Bits et Qubits

Ensemble N de bits : N^2 informations : ex : 16 bits : 2^{16}

2 bits : 00 11 01 10 : 4 états : 2^2 états
2 qubits : a |0> + b |1> → c |0> + d |1> : 2^N Informations

2^{20} : 1 048 576
1024^2 : 1 048 576

2^{60} : 1 152 921 504 606 846 97

8Go : 6,4e+10 bits → $(6{,}4e+10)^2$ = 4 096 000 000 000 000 000 000

C’est quoi un phénomène quantique ?

Quantum d’action : S avec S = Energie x Temps

Constante de Planck : h = 6,6253.10^{-34} J.s

Phénomène quantique : S < h

Papillon : 1 cm, 1 mg

A v = 1 mm.s^{-1} , S = 10^{-8} J.s >> h Phénomène classique

A v = 0 mm.s^{-1} , S = 0 << h Papillon quantique ?

C’est quoi un phénomène quantique ?

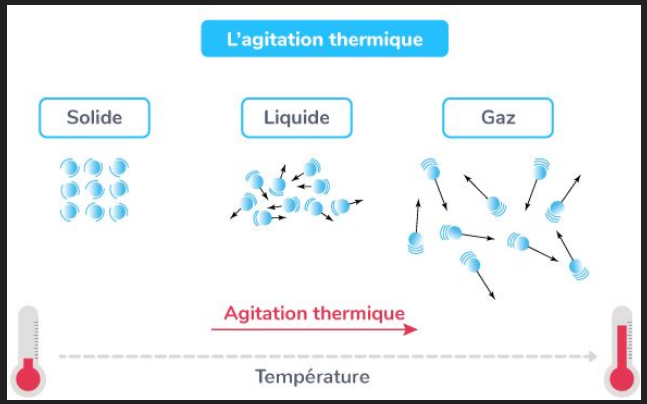
Quantum d’action : S avec S = Energie x Temps

Constante de Planck : h = 6,6253.10^{-34} J.s

Phénomène quantique : S < h

Papillon : 1 cm, 1 mg
A v = 1 mm.s^{-1} , S = 10^{-8} J.s >> h Phénomène classique
A v = 0 mm.s^{-1} , S = 0 << h Papillon quantique ?

Il faut prendre en compte l’agitation thermique !
$mv^2 = k_B T$



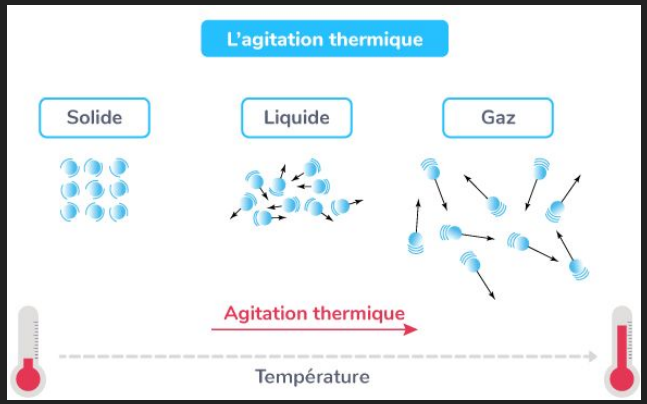
C’est quoi un phénomène quantique ?

Quantum d’action : S avec S = Energie x Temps

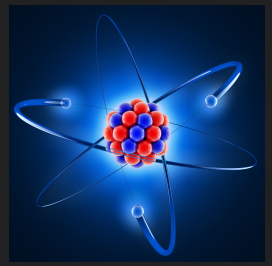
Constante de Planck : h = $6{,}6253.10^{-34}$ J.s

Phénomène quantique : S < h

Papillon : 1 cm, 1 mg
A v = 1 mm.s^{-1} , S = 10^{-8} J.s >> h Phénomène classique
A v = 0 mm.s^{-1} , S = 0 << h Papillon quantique ?

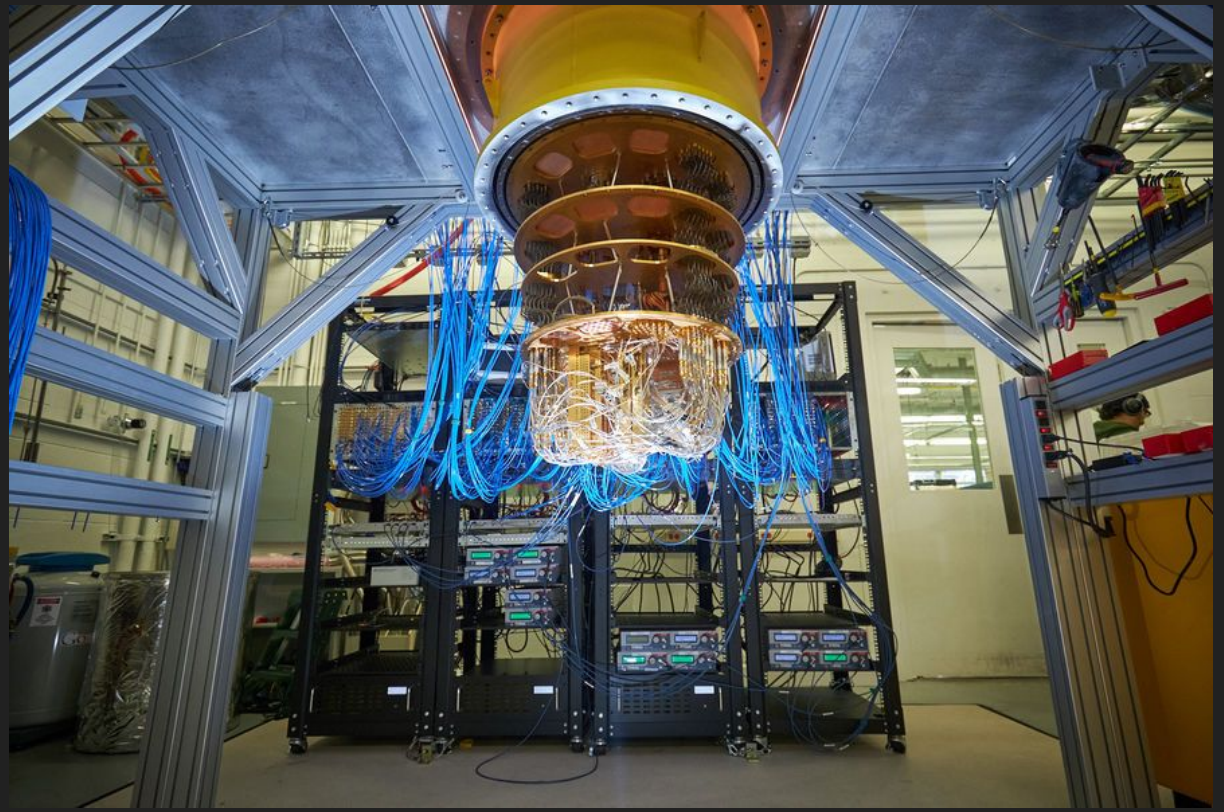


Il faut prendre en compte l’agitation thermique !
$mv^2 = k_B T$



Atome : 10^{-10} m, 10^{-27} kg
A T = 300 K , S = 10^{-15} J.s >> h Phénomène classique
A T = 10 K , S = 10^{-35} J.s ~ h Phénomène quantique !

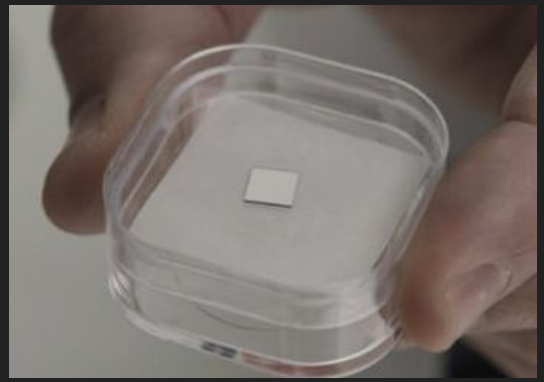
Un ordinateur quantique



Ordinateur quantique de Google

Les ordinateurs quantiques à température ambiante

La société Quantum Brillance (Australie) a créée un ordinateur quantique refroidi à température ambiante à partir de diamants imparfaits.



https://www.datacenterdynamics.com/en/news/pawsey-supercomputing-centre-installs-room-temperature-diamond-based-quantum-computer/

Références

Ordinateur quantique de Google : 53 qubits : 2^53 bits d’information

Ordinateur quantique d’IBM : 433 qubits. (10 nov 2022)

Projection d’IBM : 2025 : 4000 qubits !

Les réseaux quantiques

Principe de superposition

Chat de Schrödinger

Cryptographie quantique

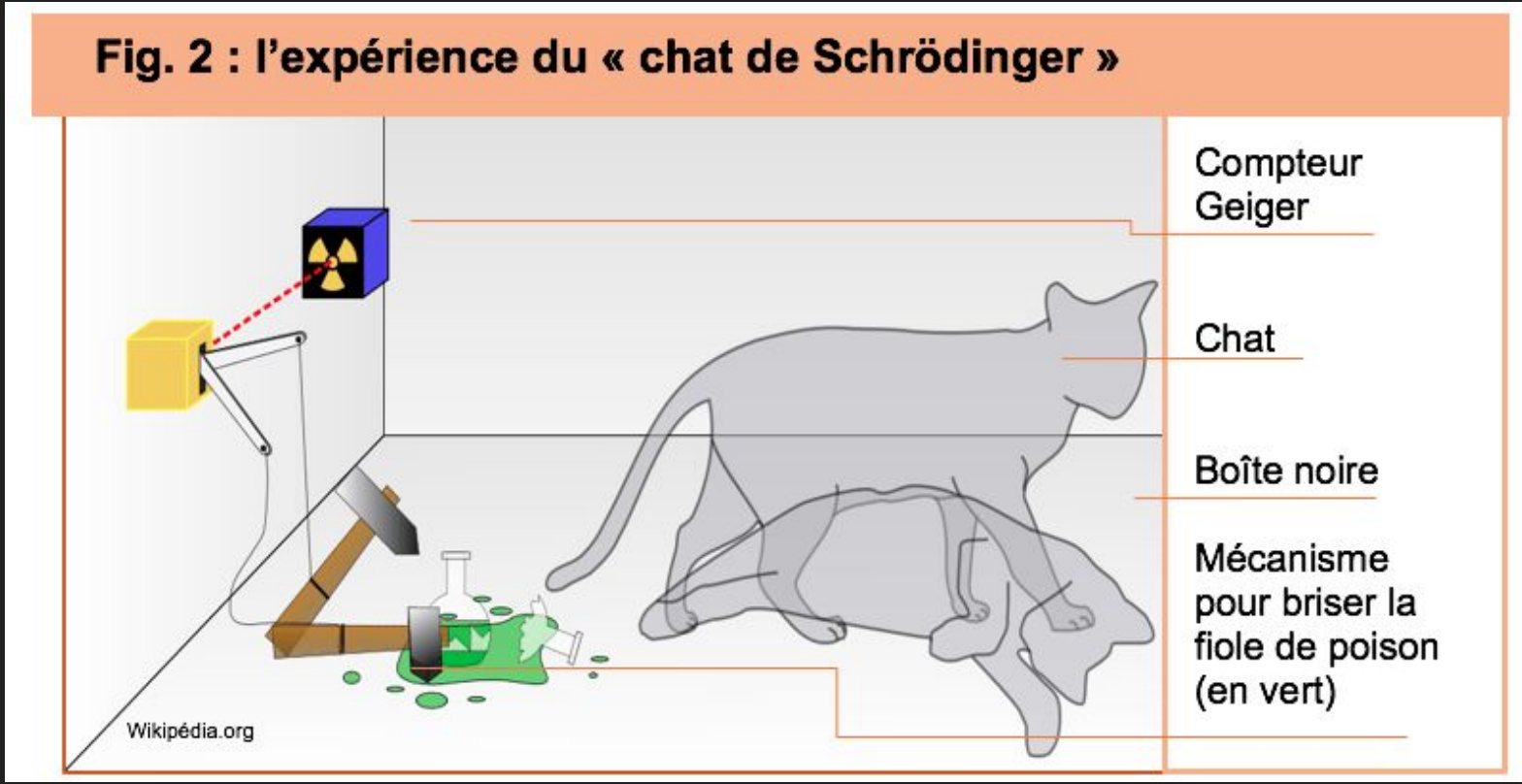
Principe de superposition

Un même état quantique peut posséder plusieurs valeurs pour une certaine quantité observable.

Dans un événement de mécanique quantique on calcule la probabilité qu'une particule se situe dans un certain état.

Tant qu'une **mesure** n'a pas été effectuée, la superposition quantique existe.

Le chat de Schrödinger



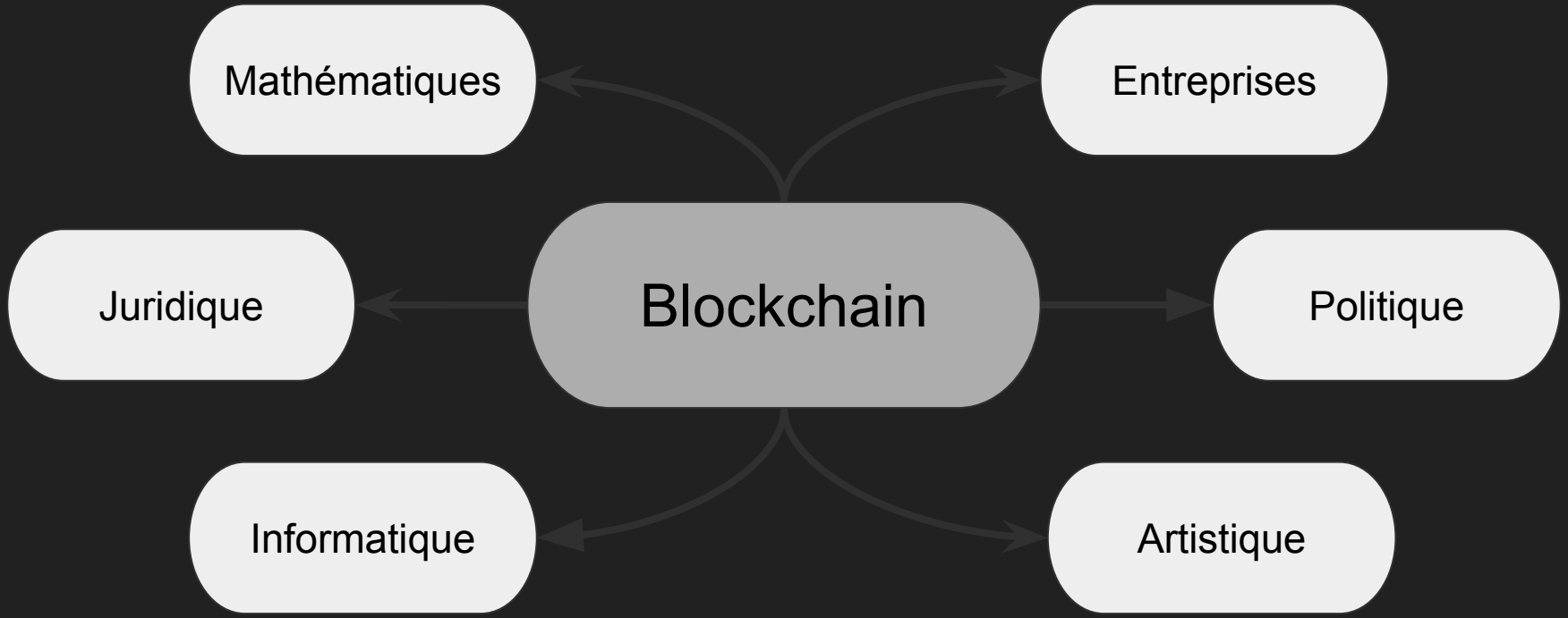
La cryptographie quantique

Si on intercepte un message entre 2 personnes, on va introduire une erreur dans ce dernier.

On va donc détecter de manière immédiate que quelqu'un tente d'accéder à la transmission.

La Blockchain

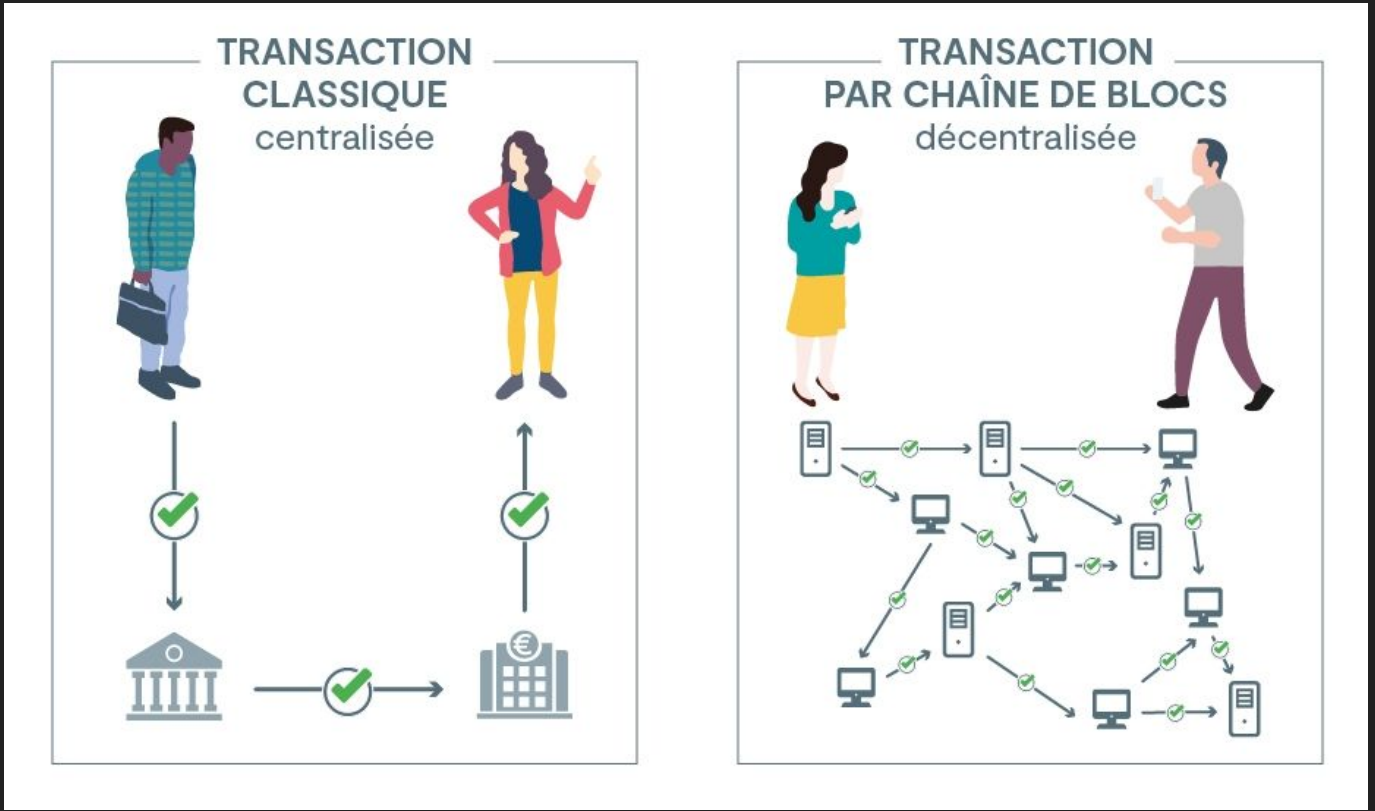
Présentation

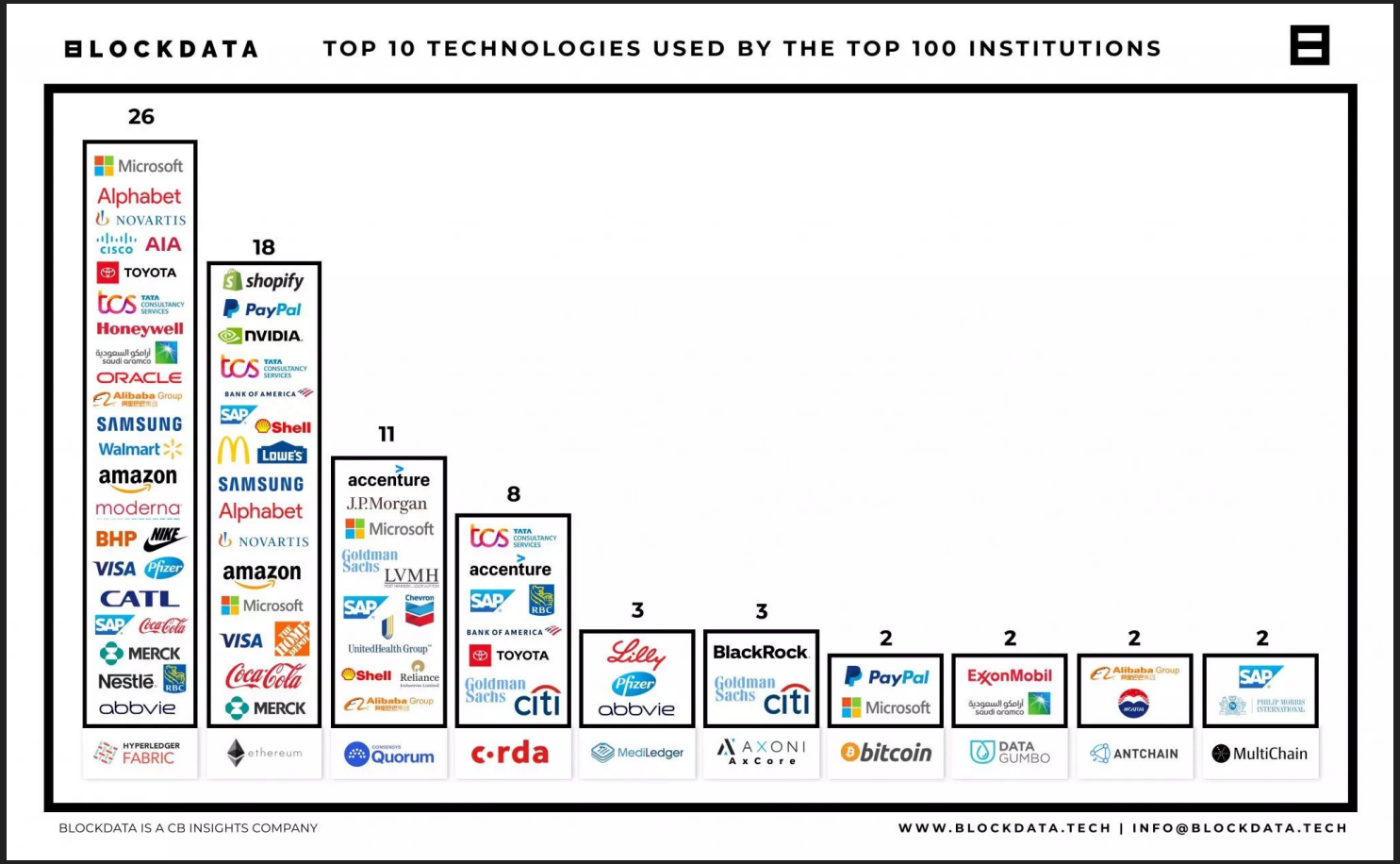


Définition

“Une chaîne de blocs (ou blockchain) est une technologie de stockage et de transmission d’informations prenant la forme d’une base de données. Elle fonctionne sans organe central de contrôle. Elle est partagée simultanément avec tous ses utilisateurs.”

Définition


TRANSACTION
CLASSIQUE
centralisée
TRANSACTION
PAR CHAÎNE DE BLOCS
décentralisée

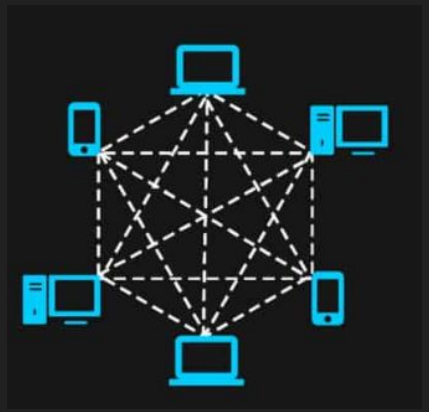


Source : Blockdata

Les blockchains publiques

Les blockchains publiques sont les premières à avoir été créées. (Notamment le protocole Bitcoin).

Ce sont celles qui ont permis de populariser la Technologie du Ledger Distribué (DLT)

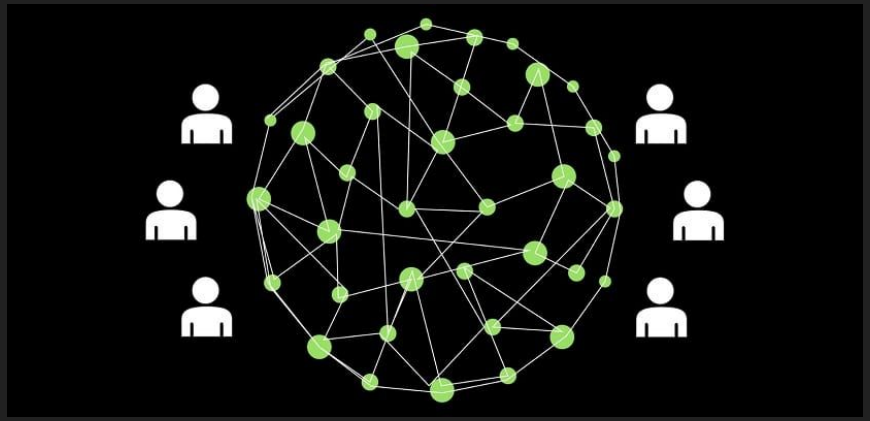


Les blockchains publiques

Définition : DLT :

Distributed Ledger Technology

Système numérique d'enregistrement des transactions de biens dans lequel les transactions et leurs détails sont enregistrés à plusieurs endroits en même temps.



Les blockchains publiques

Sa nature décentralisée exige une méthode pour vérifier l’authenticité des données.

On le fait notamment par un algorithme de consensus par lequel les participants de la Blockchain se mettent d’accord sur l’état actuel du Ledger.

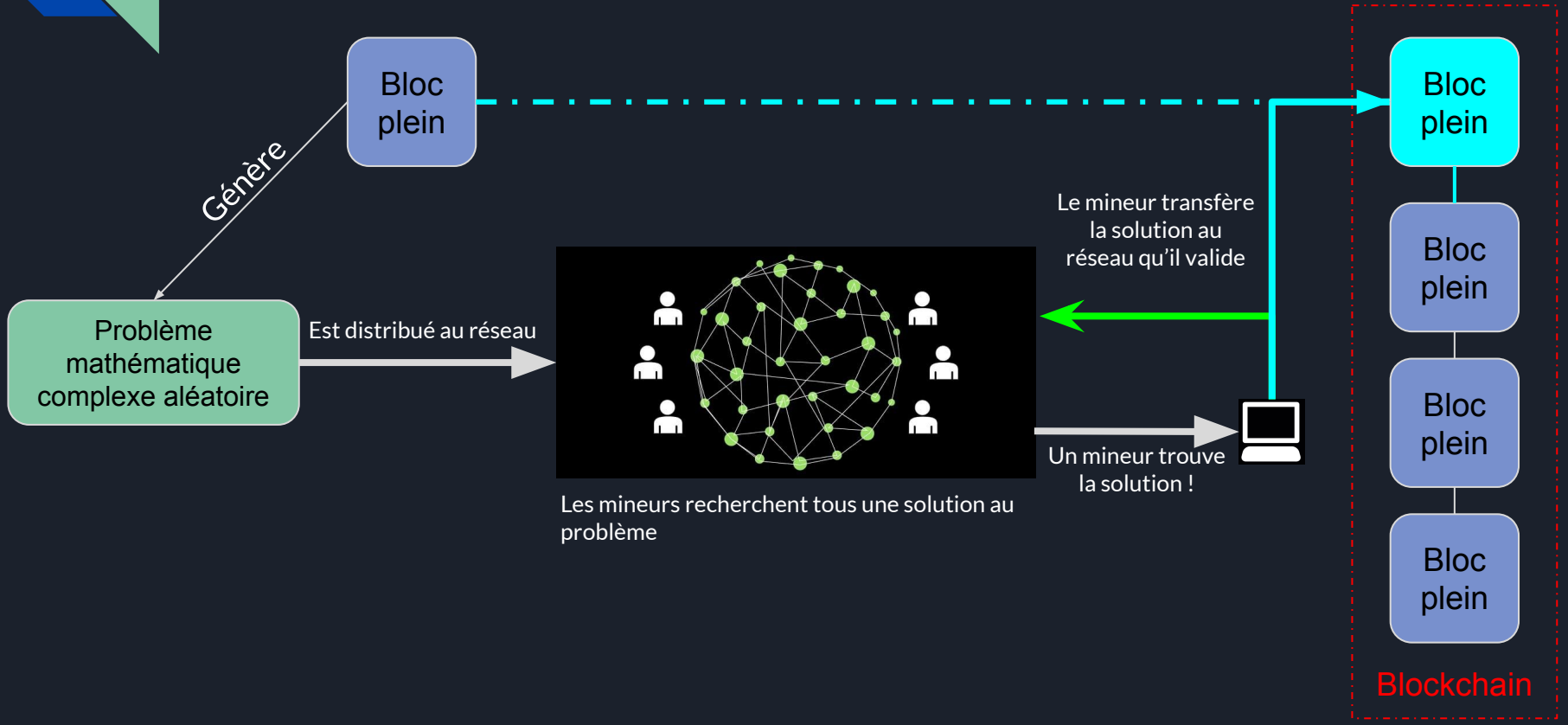
Les blockchains publiques

Il existe 2 méthodes de consensus courantes :

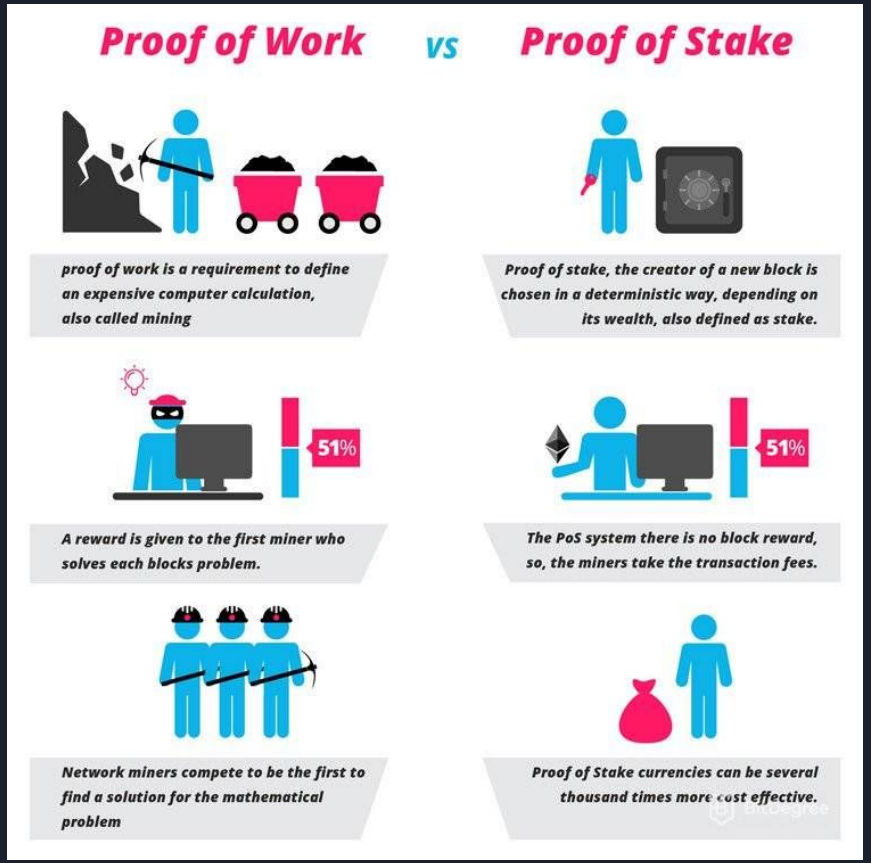
Le Proof of Work (Preuve de travail) (Bitcoin)

Le Proof of Stake (Preuve d’enjeu) (Ethereum 2.0)

Le Proof-Of-Work (PoW)



PoW vs PoS


Proof of Work
vs
Proof of Stake
proof of work is a requirement to define an expensive computer calculation, also called mining
Proof of stake, the creator of a new block is chosen in a deterministic way, depending on its wealth, also defined as stake.
51%
A reward is given to the first miner who solves each blocks problem.
51%
The PoS system there is no block reward, so, the miners take the transaction fees.
Network miners compete to be the first to find a solution for the mathematical problem
Proof of Stake currencies can be several thousand times more cost effective.

Les blockchains privées

La rapidité des blockchains privées les rend idéales pour les cas où la blockchain doit être cryptographiquement sécurisée mais où l'entité qui la contrôle ne veut pas que le public ait accès aux informations.

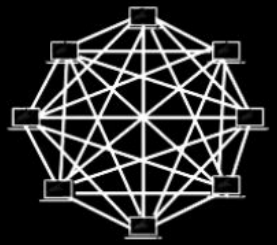
Aujourd'hui les entreprises sont de plus en plus nombreuses à adopter cette technologie.

Le meilleur exemple français reste LVMH (Louis Vuitton Moët Hennessy) pour ses produits de luxe.

Les blockchains de consortium

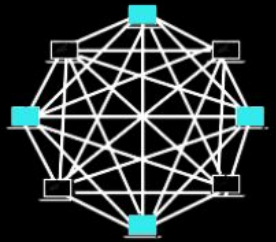
Archipels

Publique



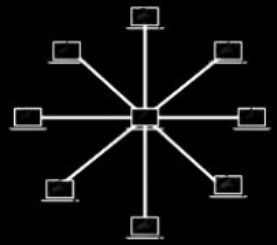
- Accessible à tout le monde, en lecture et en écriture
- Non soumise à une autorité centrale
- Tous les utilisateurs participants à la validation

Consortium



- Certains acteurs peuvent valider les transactions
- Les transactions peuvent être publiques ou limité aux participants
- Système partiellement décentralisé

Privée



- Un seul acteur peut valider les transactions
- Le système est contrôlé
- Les utilisateurs sont identifiables

AURA

AURA BLOCKCHAIN CONSORTIUM

FOUNDING MEMBERS

LVMH Mercedes-Benz OTB PRADA Group RICHEMONT

AURA Blockchain Consortium

Aura Blockchain Consortium est un rassemblement d'entreprises d'abord initié par LVMH, Prada Group, Richemont et Cartier en 2021, rejoint par la suite par OTB en octobre 2021 et Mercedes Benz en mai 2022.

L'objectif est de permettre d'authentifier les produits d'origine de ces marques en les couplant par des NFT dans des Smarts Contracts.

LUXURY AUTHENTICATION

SUPPLY CHAIN TRANSPARENCY

TRANSFER OF OWNERSHIP

PERSONAL RELATIONSHIP

CONVENIENCE & CIRCULAR ECONOMY

SUSTAINABLE BLOCKCHAIN

https://auraluxuryblockchain.com/

Aura Standard

Aura Standard is a self-managed offering for brands that care about decentralization and want control over data. The Aura Blockchain Consortium's software is run directly by the brand and the brand participates in the blockchain governance.

JOIN US

ARCHITECTURE / INFRA

- Self-managed infrastructure via Microsoft Azure ®™ subscription
- Customizable APIs & SDKs
- Self-managed data privacy

Aura SaaS

Aura SaaS is an offering for brands that want to quickly leverage the Aura Blockchain Consortium's software without the hurdle of hosting the solution. Brands use blockchain as a service without running any node.

JOIN US

ARCHITECTURE / INFRA

- SaaS offering, managed by Aura Blockchain Consortium
- Default APIs & SDKs
- Data privacy managed by Aura Blockchain Consortium

Qu’est ce qu’une crypto-monnaie ?

Qu’est ce qu’une crypto-monnaie ?

La cryptomonnaie, parfois appelée crypto-monnaie ou crypto, est une forme de monnaie qui existe sous forme numérique ou virtuelle et qui utilise la cryptographie pour sécuriser les transactions. Les cryptomonnaies n'ont pas d'autorité centrale d'émission ni de régulation, mais elles utilisent un système décentralisé pour enregistrer les transactions et émettre de nouvelles unités.

Kaspersky

Les “cryptomonnaies”, plutôt appelés “crypto-actifs” sont des actifs numériques virtuels qui reposent sur la technologie de la blockchain à travers un registre décentralisé et un protocole informatique crypté. Un crypto-actif n’est pas une monnaie. Sa valeur se détermine uniquement en fonction de l’offre et de la demande. Les crypto-actifs ne reposent pas sur un tiers de confiance comme une banque centrale pour une monnaie.

Autorité des marchés financiers (AMF)

Qu’est ce qu’une crypto-monnaie ?

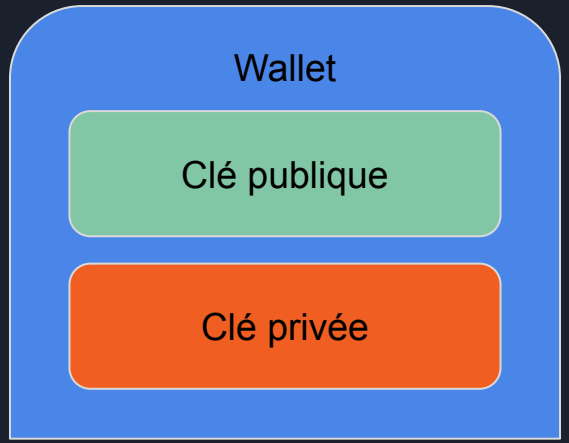
“Moyen de paiement virtuel utilisable essentiellement sur Internet, s’appuyant sur la cryptographie pour sécuriser les transactions et la création d’unités, et échappant à tout contrôle des régulateurs et des banques centrales. (On dit aussi *monnaie cryptographique*.) [il existe des centaines de cryptomonnaies dans le monde, parmi lesquelles le bitcoin. Parce qu’elles sont dépourvues de cours légal, les spécialistes privilégient l’appellation *cryptoactifs*.]” Larousse

Stockage et utilisation

Le stockage de crypto-actifs se fait via des portefeuilles qu'on appelle "wallets".

Certains peuvent stocker plusieurs crypto-actifs et d'autres un seul.

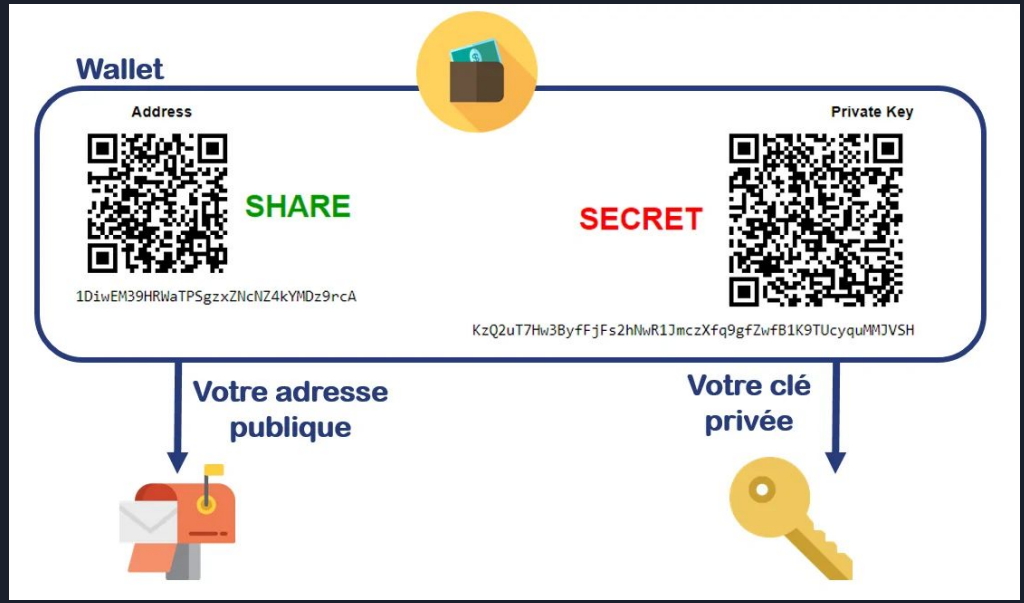
Ces derniers sont dotés de 2 éléments qu'on nomme "clé publique" et "clé privée".



Stockage et utilisation

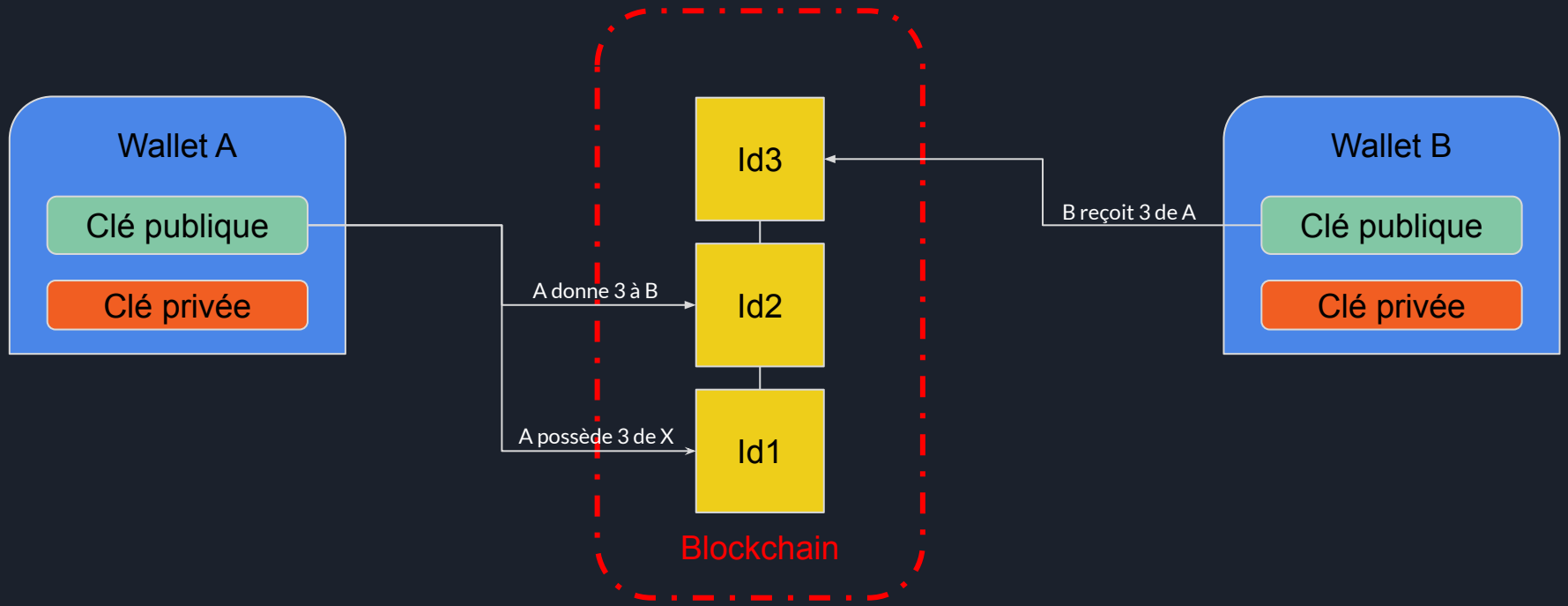
La clé publique représente votre nom, c'est celle qui va permettre d'identifier les transactions sur la blockchain et de vous envoyer des crypto-actifs. Elle permet également de retrouver l'intégralité des transactions liées à votre wallet.

La clé privée agit comme un mot de passe, qui permet d'avoir accès aux fonds présents sur le wallet.



Stockage et utilisation

Les crypto-actifs ne quittent jamais la blockchain, les échanges se faisant entre portefeuilles, la quantité de crypto-actifs ne change que de clé.



Entreprises & Crypto-Actifs

Samsung Blockchain

Samsung Blockchain permet de stocker, envoyer et recevoir des crypto-actifs

PayPal x ConsenSys (Metamask)

Démonstration : Etherscan & APE BOARD

ETHERSCAN

The Ethereum Block Explorer

Le contrôle et les régulations

Européen

Règlement MiCA (Market in Crypto-Assets)

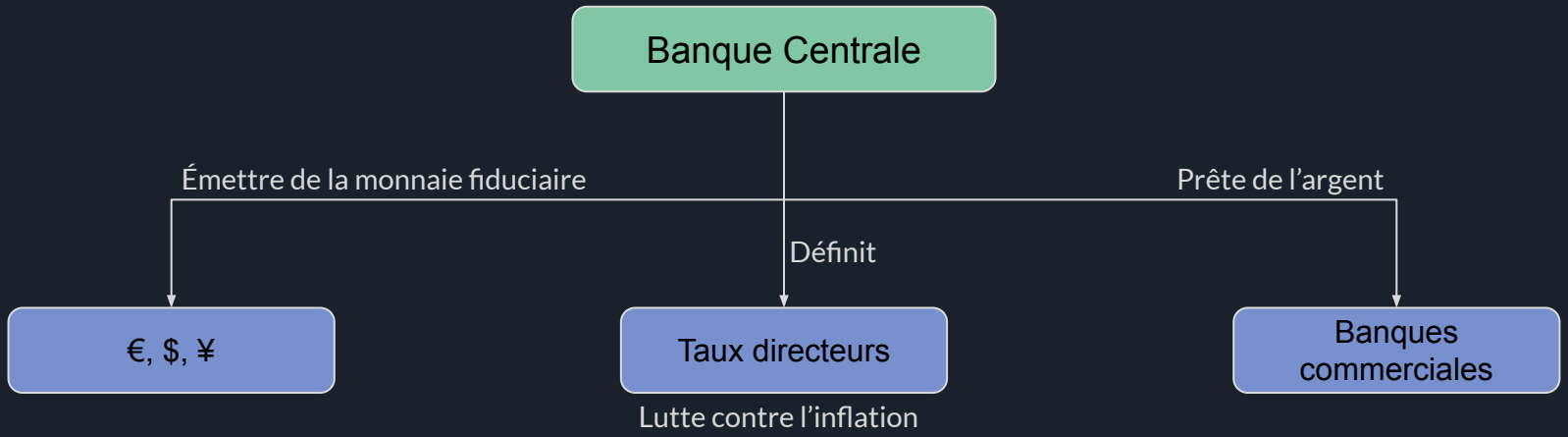
Français

Enregistrement auprès de l'AMF

PSAN : Prestataire de Services sur Actifs Numériques

Le positionnement des banques centrales

Aujourd'hui le positionnement des banques centrales (FED, BCE, BPC) ne sont pas contre les crypto-actifs mais contre leur décentralisation et leur non régulation.

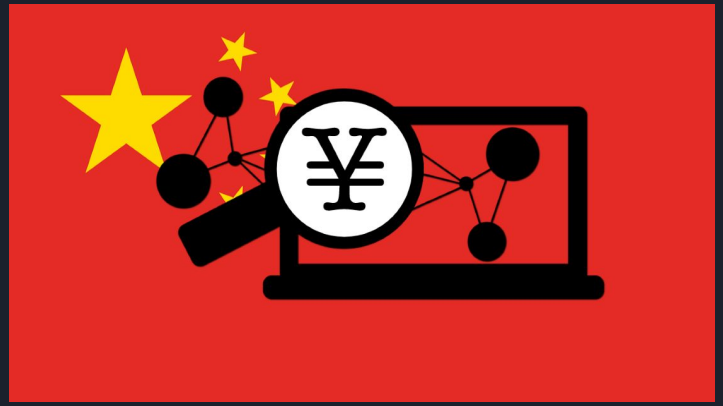


Les MNBC

Les monnaies numériques de banque centrale (ou MNBC) sont une version numérique des espèces. On parle d’ailleurs aujourd'hui d'Euro Numérique ou de Yuan Numérique.

Les MNBC

La Chine est un excellent exemple car elle a rendu illégale l'utilisation et la transaction de crypto-actifs en 2021 mais développe en parallèle son Yuan Numérique dont les tests ont débuté en avril 2022.

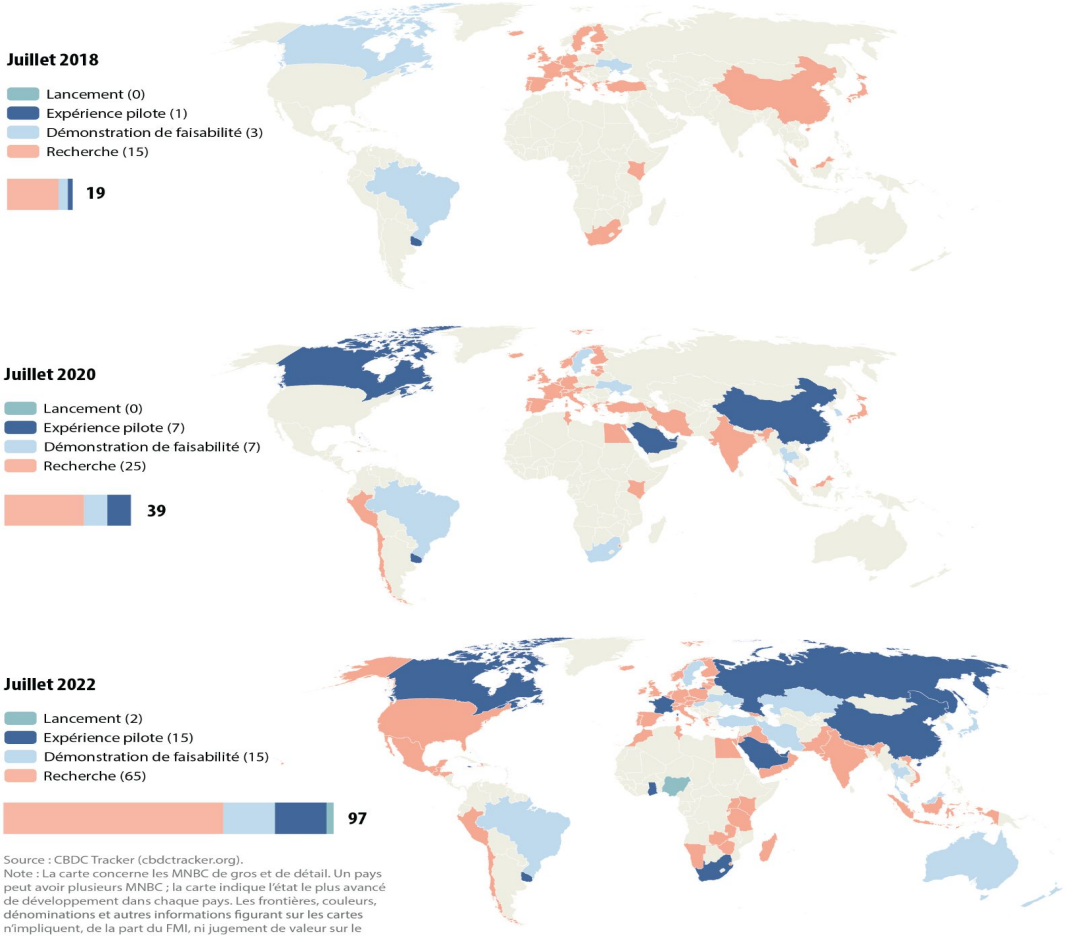


Les MNBC

Le gouverneur de la banque de France a annoncé un déploiement de l'Euro numérique dans les années 2027-2028 lors d'une conférence en septembre 2022.

Cartographie des MNBC

Les banques centrales passent par divers stades de développement pour évaluer les avantages et les risques des MNBC et réfléchir à la meilleure façon de les déployer (stades de développement des MNBC par pays pour la période indiquée)



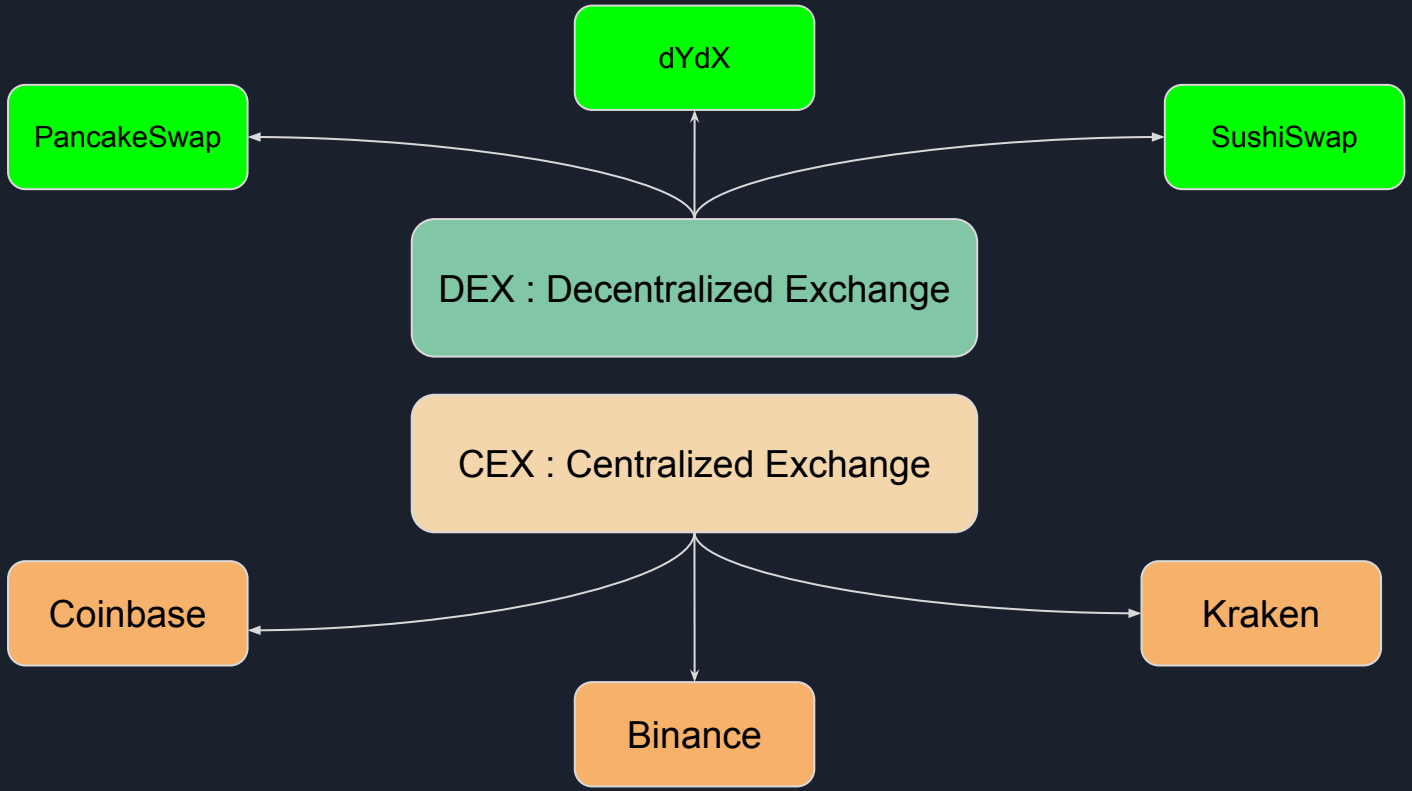
Source : CBDC Tracker (cbdctracker.org).
Note : La carte concerne les MNBC de gros et de détail. Un pays peut avoir plusieurs MNBC ; la carte indique l'état le plus avancé de développement dans chaque pays. Les frontières, couleurs, dénominations et autres informations figurant sur les cartes n'impliquent, de la part du FMI, ni jugement de valeur sur le statut juridique d'un territoire, ni reconnaissance ou approbation de ces frontières.

DEX vs CEX

DEX : Decentralized Exchange

CEX : Centralized Exchange

DEX vs CEX


dYdX
PancakeSwap
SushiSwap
DEX : Decentralized Exchange
CEX : Centralized Exchange
Coinbase
Kraken
Binance

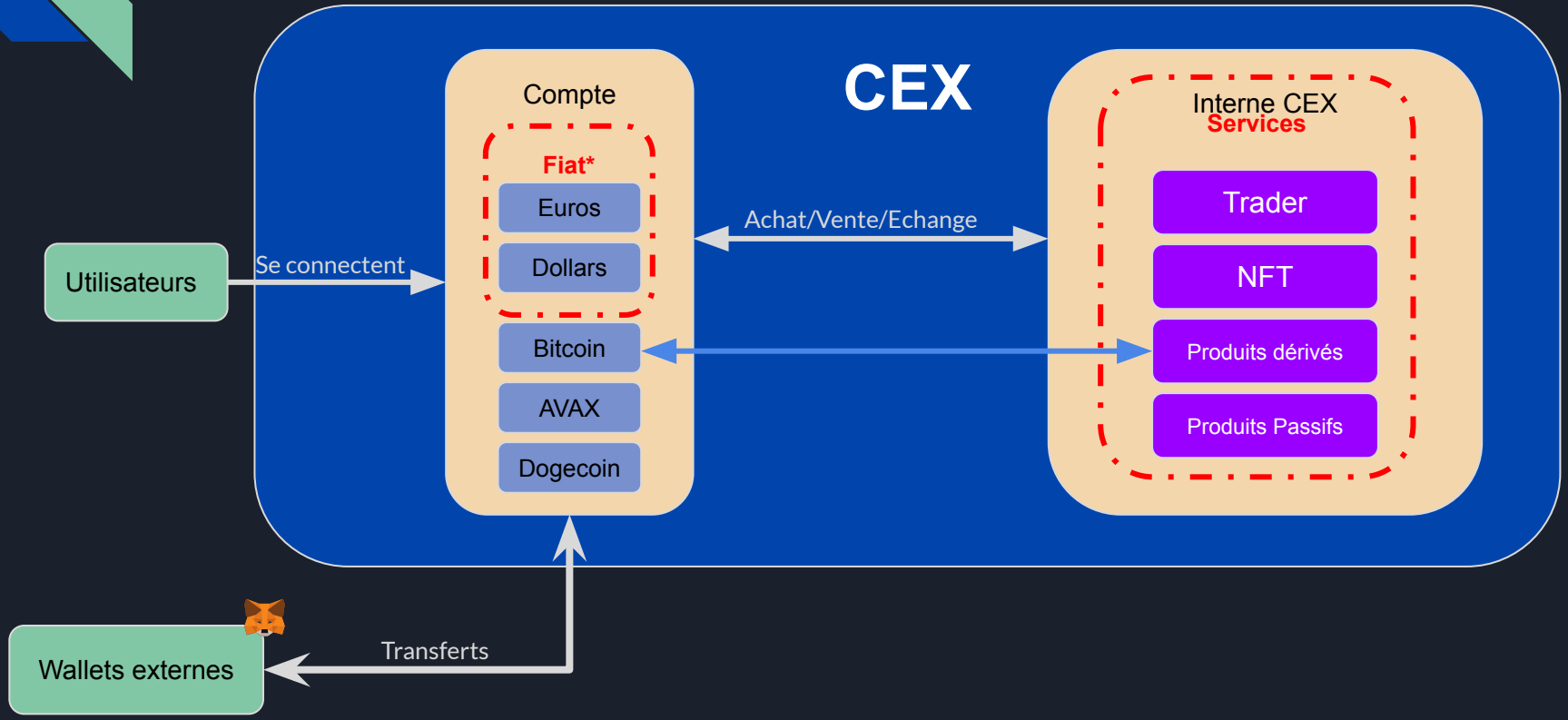
Les CEX (Centralized EXchanges)

Les CEX sont des entreprises qui disposent d'une plateforme Web afin de pouvoir effectuer des échanges entre crypto-actifs de différentes blockchains ou d'une même blockchain.

Il existe un grand nombre de choix de crypto-actifs qui sont dits "listés" sur les plateformes d' échange.

Le KYC est obligatoire dans la politique des CEX. (respect des réglementations).

Les CEX (Centralized EXchanges)



*"Fiat" = "Décret"

Les CEX (Centralized EXchanges)

Ranking CoinMarketCap des CEX 2023 (février)

Top 10				
	Binance	bitFlyer	BitMart	Coinone
	Coinbase Ex	Bitget	Upbit	CoinW
	Kraken	Bybit	Korbit	Coinsbit
	KuCoin	Gate.io	ProBit Global	bitMEX
	Bitfinex	LBank	Binance TR	P2B
	Bitstamp	Crypto.com	BTCEX	Hotcoin Global
	Binance US	MEXC	Bitrue	Phemex
	OKX	Huobi	Bittrex	Bitso
	Bithump	Coincheck	Zaif	Okcoin
	Gemini	BKEX	Poloniex	BingX

https://coinmarketcap.com/fr/rankings/exchanges/

Binance

Binance est aujourd'hui le plus gros exchange centralisé du monde.

2022 : 90 millions d'utilisateurs

Volume journalier d'échange : 90M $

Année de création : 2017

Maison mère : Hong Kong

Chiffre d'affaires : ?

Coinbase

- Introduite et cotée en bourse (NASDAQ:COIN) en 2019
- 2022 : ~ 80 millions d’utilisateurs
- Volume journalier d’échange : 1,8M $
- Année de création : 2012
- Maison mère : San Francisco
- Chiffre d'affaires (2020) : 1,2M $

Coinbase

Fondateurs

Brian Armstrong

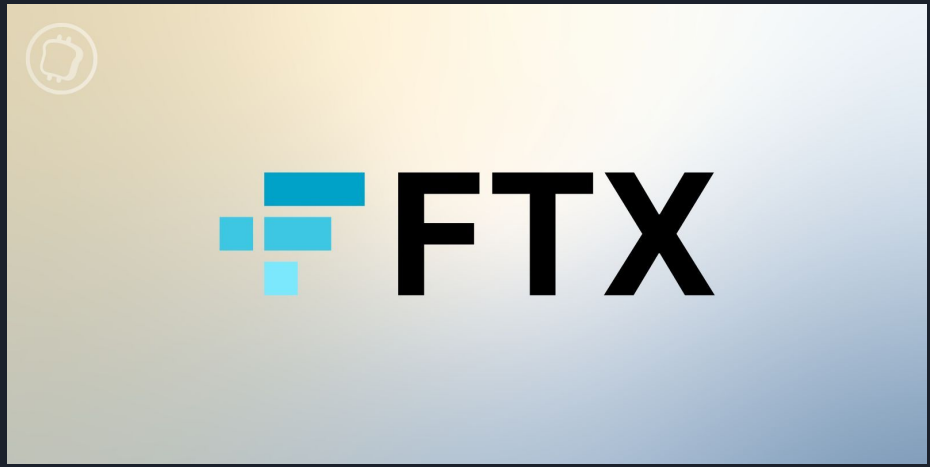
Fred Ehrsah

FTX

FTX fut le 2ème plus grand exchange de crypto-actifs au monde avec une valorisation à 14 milliards de dollars.

Son CEO Sam Bankman-Fried est actuellement sous le feu des projecteurs pour avoir détourné l'argent de ses utilisateurs à des fins personnelles.

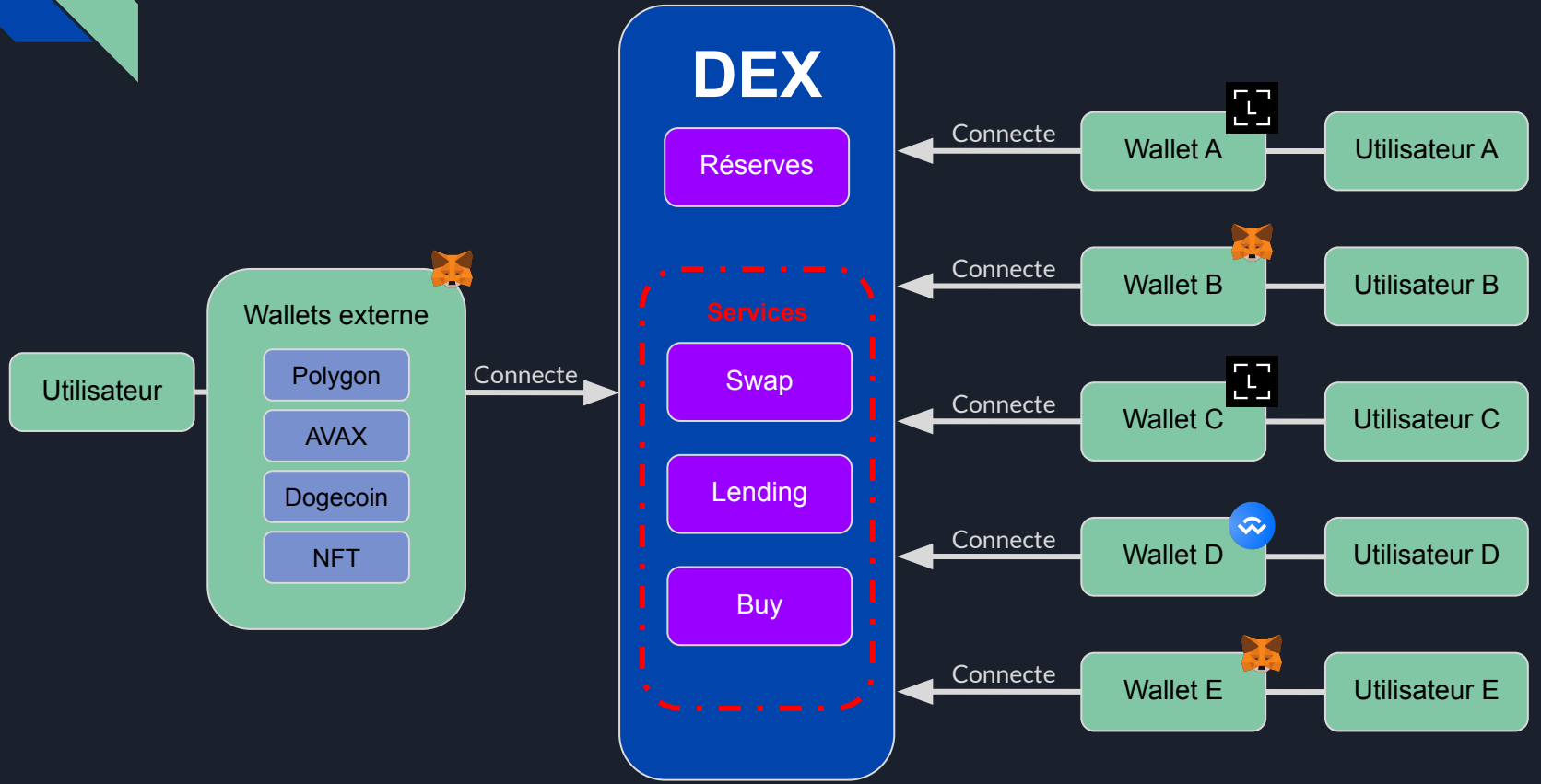
Le procès est actuellement en cours.



Les DEX (Decentralized EXchanges)

Les principaux concurrents des CEX sont les DEX. Sur ces plateformes, les utilisateurs peuvent s’échanger directement leurs actifs numériques sans les avoir déposés sur les plateformes. Il suffit de posséder un Wallet externe qu’on vient connecter sur un DEX.

Les DEX (Decentralized EXchanges)



PancakeSwap

DEX construit sur la BSC (Binance Smart Chain)

Créé en 2020

Volume de transaction en milliards de dollars par jour.

Frais de transaction bas.

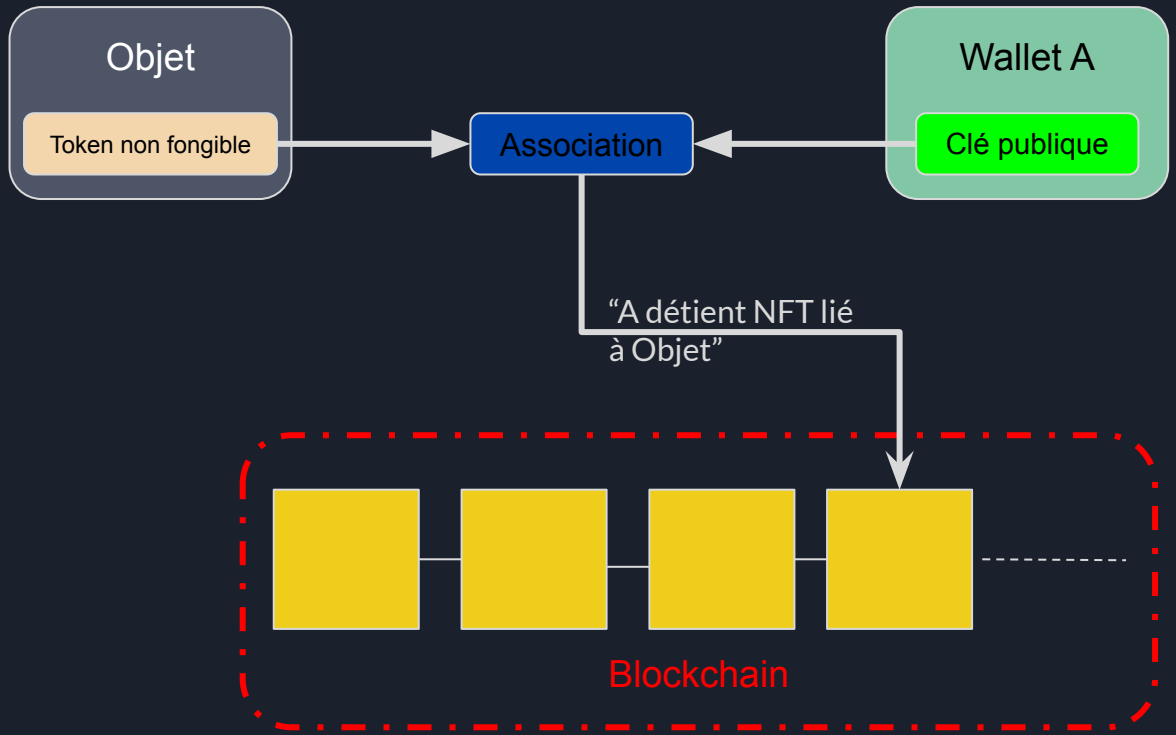
Qu’est ce qu’un NFT ?

Un NFT pour “Non-Fungible Token” est un jeton dit non fongible ou encore non interchangeable.

Dans le cas de la monnaie classique, toute pièce ou tout billet est interchangeable.

Cela permet de créer une propriété numérique authentique et unique vérifiable sur la Blockchain.

Qu’est ce qu’un NFT ?



OpenSea

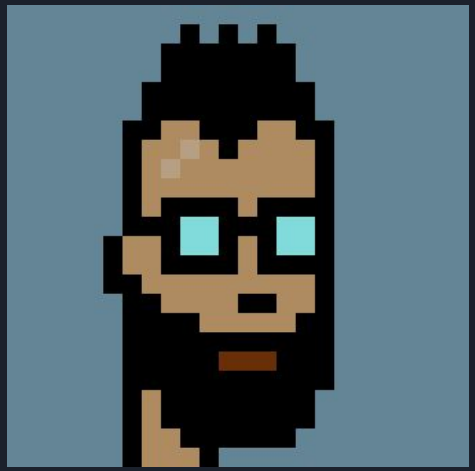
OpenSea est aujourd'hui la plus grande plateforme d'échange de NFT au monde.

Elle repose sur la Blockchain Ethereum.

On la considère comme la marketplace de référence.

Vision Publique - les NFT dans l’Art

Mutant Ape Yacht Club #12456
Collection Mutant Ape Yacht Club
Prix : 15,72Eth
(~22 700 €)
https://opensea.io/fr/assets/ethereum/0x60e4d786628fea6478f785a6d7e704777c86a7c6/12456



Cryptopunk #1001
Collection CryptoPunks
Prix : 110Eth
(~158 000 €)
https://opensea.io/fr/assets/ethereum/0xb47e3cd837ddf8e4c57f05d70ab865de6e193bbb/1001

Les NFT dans l'Art

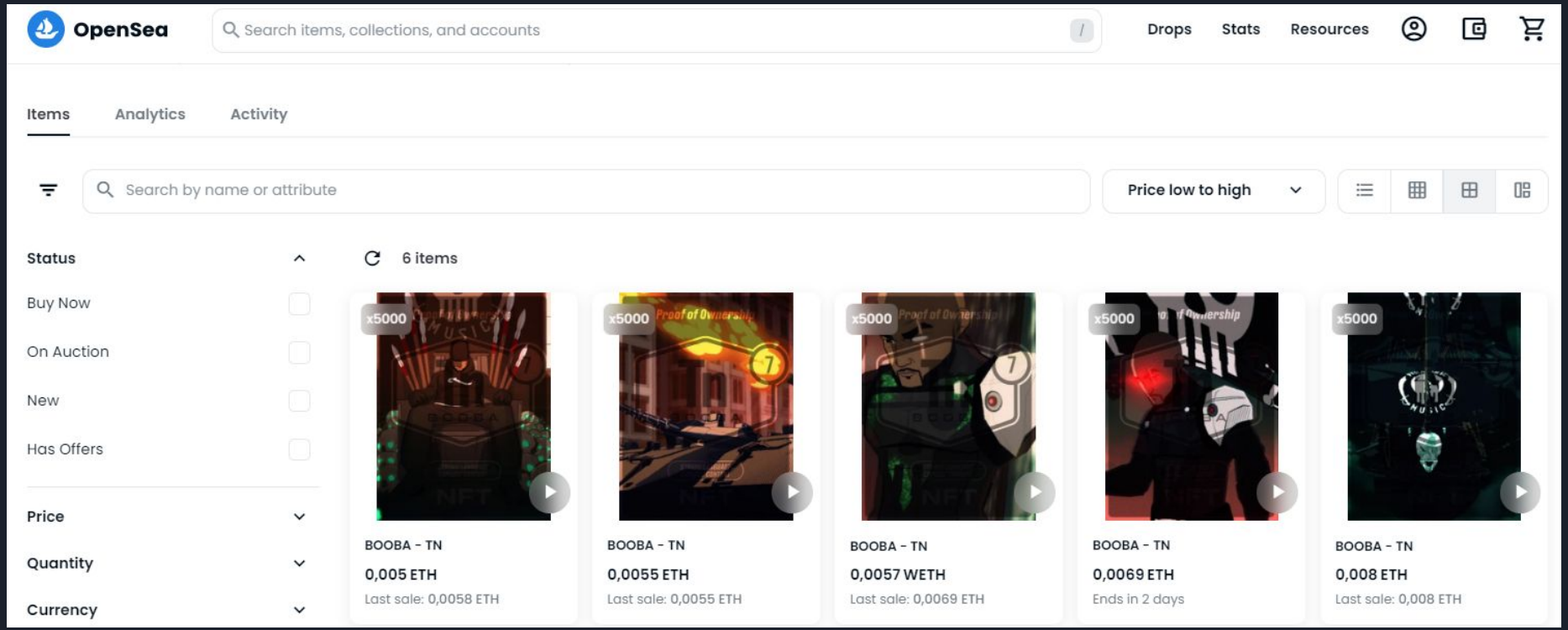
Aujourd'hui, de nombreux musées comme l'Hermitage, le Louvre, le British Museum se sont mis à vendre leurs œuvres sous forme de NFT.

Reproduction NFT d'un tableau de Raphaël, à Londres (Royaume-Uni), le 15 février 2022. JUSTIN TALLIS / AFP

La Vierge du Chardonneret

Les NFT dans l’Art

Les NFT dans l'Art



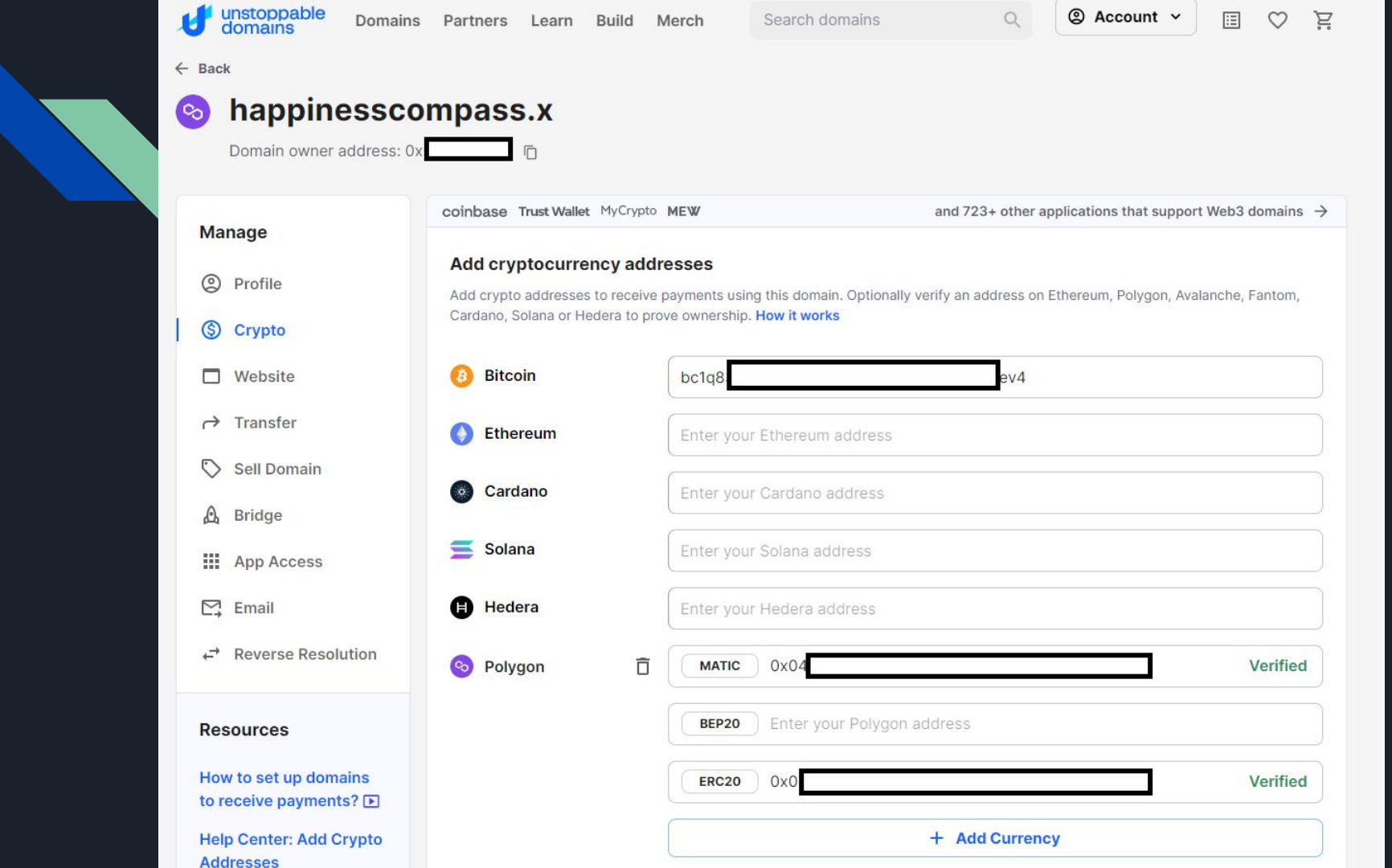
Les NFT d’art & NFT techniques

Au-delà de l’art et de la vision publique des NFT popularisés par les collections Bored Apes et Crypto Punks, on retrouve des projets visant à développer le web 3.0.

Unstoppable Domains

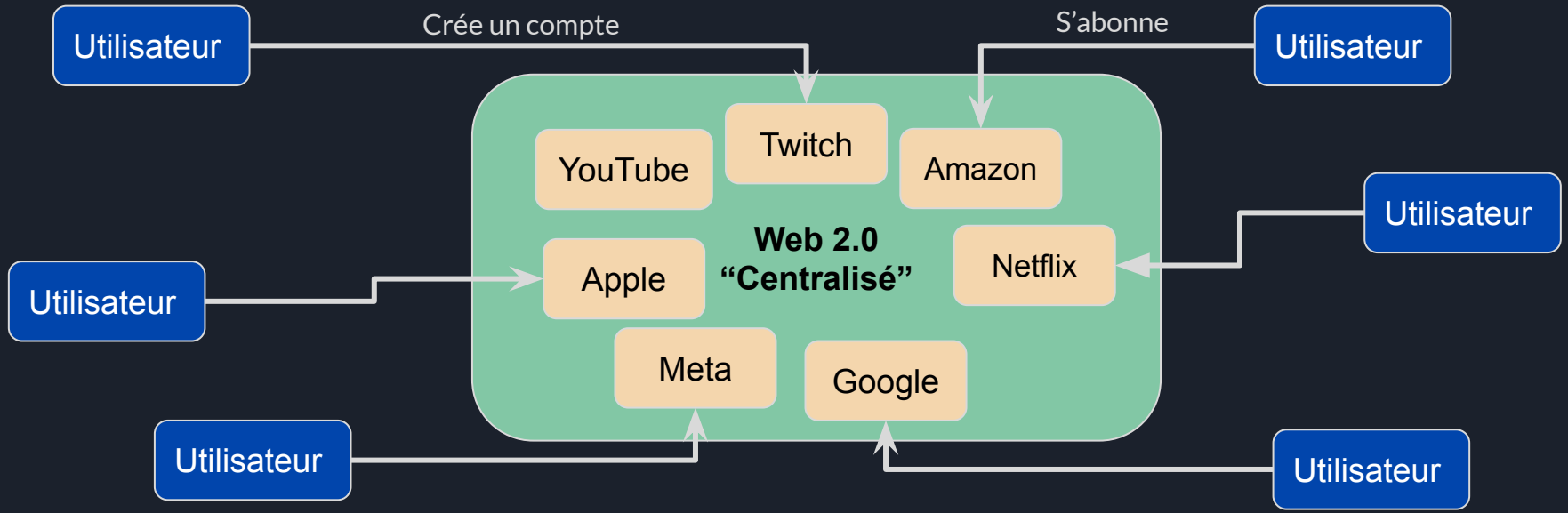
Unstoppable Domains est une entreprise qui travaille dans le Web 3.0 et qui permet d'acheter des noms de domaine uniques sous la forme de NFT.

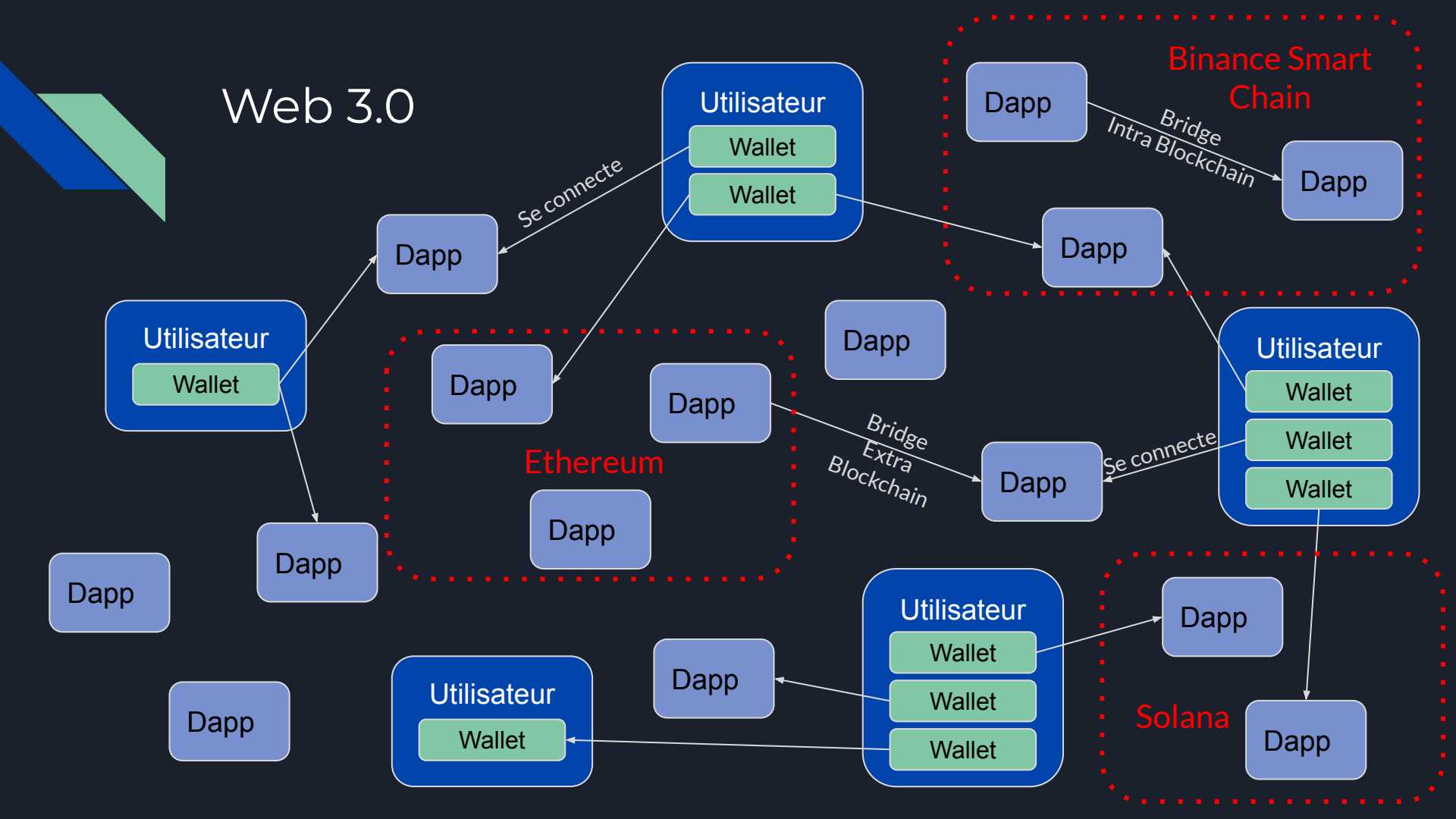
On peut venir héberger son site web dans la blockchain sous la forme d'un NFT.


unstoppable domains
Domains
Partners
Learn
Build
Merch
Search domains
Account
Back
happinesscompass.x
Domain owner address: 0x
Manage
Profile
Crypto
Website
Transfer
Sell Domain
Bridge
App Access
Email
Reverse Resolution
Resources
How to set up domains to receive payments?
Help Center: Add Crypto Addresses
coinbase
Trust Wallet
MyCrypto
MEW
and 723+ other applications that support Web3 domains
Add cryptocurrency addresses
Add crypto addresses to receive payments using this domain. Optionally verify an address on Ethereum, Polygon, Avalanche, Fantom, Cardano, Solana or Hedera to prove ownership. How it works
Bitcoin
bc1q8
ev4
Ethereum
Enter your Ethereum address
Cardano
Enter your Cardano address
Solana
Enter your Solana address
Hedera
Enter your Hedera address
Polygon
MATIC
0x04
Verified
BEP20
Enter your Polygon address
ERC20
0x0
Verified
Add Currency

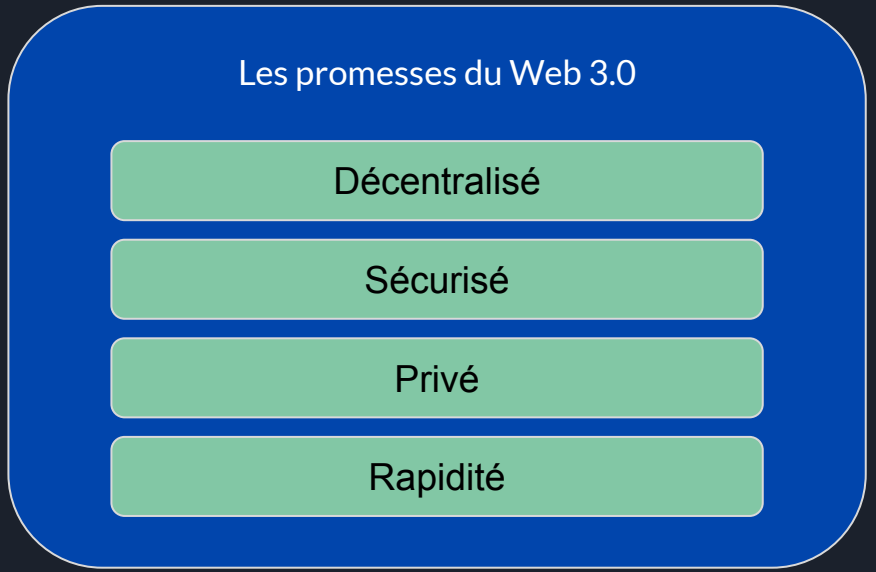
Web 3.0 - Objectif et réalité

Le Web 3.0 doit succéder au web 2.0 comme plateforme décentralisée de l'internet.

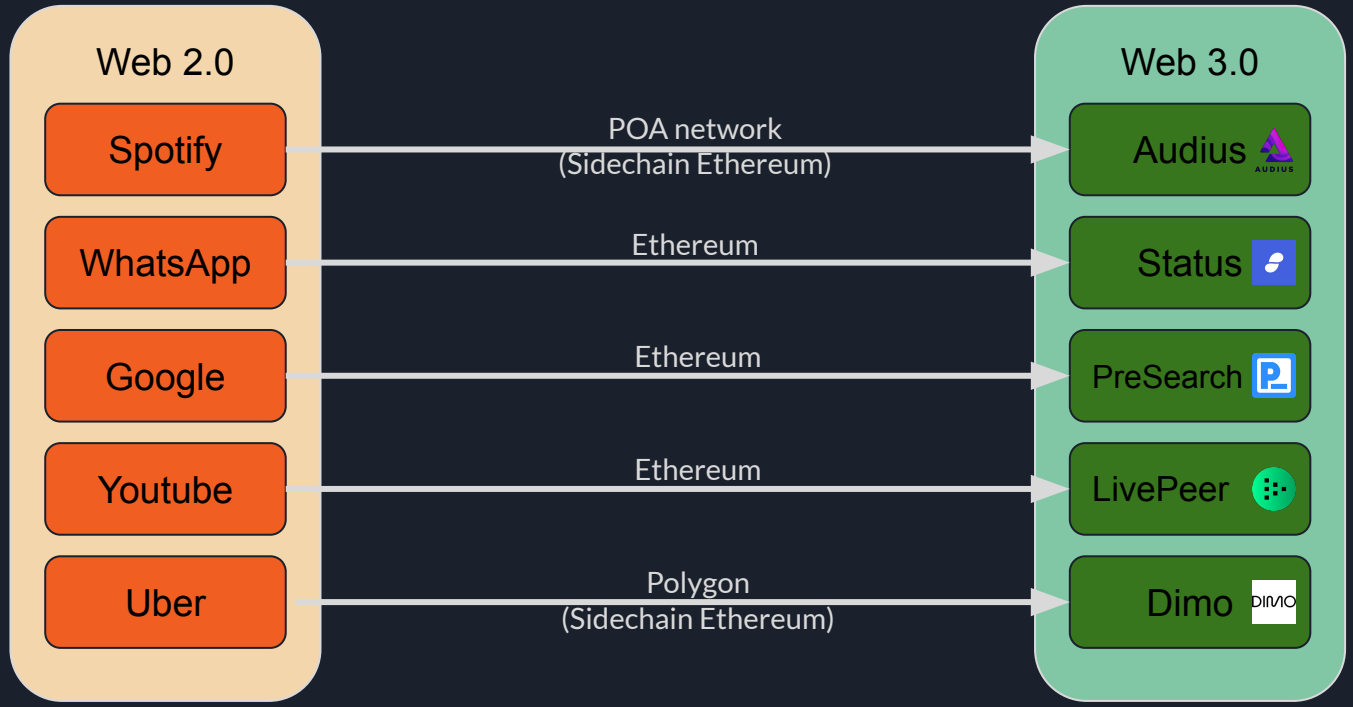



Web 3.0
Utilisateur
Wallet
Wallet
Se connecte
Dapp
Dapp
Binance Smart Chain
Dapp
Bridge
Intra Blockchain
Dapp
Dapp
Utilisateur
Wallet
Dapp
Dapp
Dapp
Ethereum
Dapp
Bridge
Extra
Blockchain
Dapp
Se connecte
Utilisateur
Wallet
Wallet
Wallet
Dapp
Dapp
Dapp
Utilisateur
Wallet
Wallet
Wallet
Dapp
Utilisateur
Wallet
Dapp
Solana
Dapp

Web 3.0 - Objectif et Réalité



Web 2.0 versus Web 3.0



Polygon - Une sidechain d'Ethereum prometteuse

Au Consumer Electronics Show (CES) de Las Vegas, Mastercard annonce choisir Polygon pour délivrer des NFT pour les producteurs musicaux dans le web 3.0